SOPHOS
Security made simple.

Il deep learning di Intercept X

Intercept X offre la combinazione ideale di deep learning e tecnologie antiexploit di primissima categoria, unite all'antiransomware CryptoGuard, a funzionalità di root cause analysis e altro ancora, per offrire la soluzione di protezione endpoint più completa che sia attualmente disponibile sul mercato. Questa combinazione esclusiva di funzionalità permette a Intercept X di bloccare il più vasto spettro di minacce endpoint.

Caratteristiche principali

- Il motore di rilevamento antimalware numero uno in termini di performance
- Prevenzione sia del malware complesso che di quello inedito
- Blocco del malware prima che riesca a eseguirsi
- Rilevamento signatureless
- Protezione anche in caso di host off-line
- Rilevamento del malware in circa 20 millisecondi
- Analisi basata su centinaia di milioni di campioni
- Efficacia comprovata su VirusTotal sin da agosto 2016
- Classificazione dei file come malevoli, app potenzialmente indesiderate (PUA) o innocui
- Subito pronta per l'uso, senza bisogno di ulteriore analisi
- Impatto minimo (meno di 20 MB)
- Particolare attenzione ai file PE (Portable Executable)

La maggior parte delle soluzioni di sicurezza utilizzate fino ad oggi sono reattive ma a volte un po' troppo lente. Con il constante aumento del volume e della complessità degli attacchi rivolti agli endpoint, gli approcci precedenti hanno fatto fatica a tenere il passo. Ad esempio, i SophosLabs analizzano più di 400.000 nuovi campioni di malware ogni giorno. Per complicare ulteriormente questo problema, i SophosLabs hanno notato che il 75% del malware riguarda un'unica organizzazione.

Il deep learning, una forma avanzata di machine learning, ci sta aiutando a cambiare il nostro approccio alla sicurezza endpoint, e Intercept X è il sistema che ci sta portando verso il futuro. Grazie all'integrazione del deep learning, Intercept X sta rivoluzionando la sicurezza endpoint, portandola da un modello reattivo a un approccio predittivo alla protezione contro le minacce inedite.

Il deep learning rispetto ad altri tipi di machine learning

"Intercept X sfrutta una rete neurale di deep learning che agisce in maniera simile al cervello umano... I risultati sono un migliore tasso di precisione sia per il malware attuale che per quello del giorno zero, nonché una percentuale minore di falsi positivi".

ESG Lab Report, dicembre 2017

Anche se molti vendor sostengono di utilizzare il machine learning, non tutti i tipi di machine learning sono uguali. Sophos utilizza il deep learning per rilevare il malware. Definito anche con i termini "reti neurali di deep learning" o semplicemente "reti neurali", il deep learning è stato ispirato dal funzionamento del cervello umano. È lo stesso tipo di machine learning frequentemente utilizzato per il riconoscimento facciale, per l'elaborazione dei linguaggi naturali, per i veicoli autonomi e per altri campi avanzati nell'ambito dell'informatica e della ricerca.

Il deep learning si è costantemente dimostrato più efficace rispetto ad altri modelli di machine learning (inclusi foreste casuali, clustering con k-mean o reti bayesiane), ma richiede grandi quantità di dati e un'enorme potenza di calcolo per poter impostare un modello efficace. Sophos ha semplificato il tutto, grazie alle attività di raccolta e analisi del malware dei SophosLabs degli ultimi 30 anni e ai dati di telemetria che riceviamo ogni giorno dai più di 100 milioni di endpoint che proteggiamo.

Il deep learning di Intercept X

Il deep learning presenta diversi vantaggi intrinsechi, rispetto agli altri tipi di machine learning comunemente utilizzati nella sicurezza endpoint:

È più intelligente: i modelli di deep learning elaborano i dati su livelli di analisi multipli, proprio come i neuroni nel cervello umano. A ogni livello, il modello diventa notevolmente più potente. Analizza relazioni complesse tra funzionalità di input diverse. In questo modo, è in grado di scoprire e applicare automaticamente la migliore combinazione di input, con un processo decisionale che sarebbe impossibile per gli esseri umani. Ciò significa che il modello di rilevamento antimalware basato sul deep learning di Sophos sarà in grado di rilevare malware che passerebbe inosservato agli occhi degli altri motori di machine learning.

È più scalabile: Il deep learning si adatta in maniera elegante a centinaia di milioni di campioni analizzati. È importante sottolineare che ogni settimana i SophosLabs analizzano 2,8 milioni di nuovi campioni di malware. Poiché può continuare a ricevere quantità enormi di dati da analizzare, il nostro modello è in grado di "memorizzare", durante il processo di analisi, l'intero panorama visibile delle minacce. Siccome può elaborare una quantità di input considerevolmente superiore, il deep learning è in grado di predire con maggiore precisione le minacce attuali, pur continuando a mantenersi aggiornato con il passare del tempo:

È più leggero: I tradizionali approcci al machine learning generano modelli di dimensioni molto elevate, che a volte possono occupare diversi gigabyte sul disco. A differenza di questi, l'approccio di deep learning di Sophos crea modelli molto compressi. Il modello di deep learning di Sophos è piccolissimo, con meno di 20 MB sull'endpoint e un impatto sulla performance quasi pari a zero.

Le capacità di deep learning di Sophos

Sophos vanta alti livelli di esperienza nell'ambito del deep learning e offre il motore di rilevamento antimalware con la migliore performance del settore:

Esperienza: A differenza dei nostri competitor, siamo esperti di machine learning per la cybersecurity da molto tempo. Inoltre, i nostri modelli di rilevamento antimalware basato sul deep learning sono operativi in ambienti di produzione da diversi anni. Il modello di rilevamento antimalware di Sophos è stato realizzato dal nostro team di esperti di data science con tecnologie DARPA. Nel 2010, l'American Defense Advanced Research Projects Agency (DARPA) ha realizzato il Cyber Genome Program per rivelare il "DNA" del malware e di altre minacce informatiche. Si trattava delle origini di quello che oggi è l'algoritmo integrato in Intercept X.

Affidabilità: Siamo sempre stati trasparenti in merito ai nostri modelli. Oltre a presentare i dettagli della nostra metodologia agli eventi di settore, come ad es. Black Hat, non ci siamo neppure negati ai test realizzati da laboratori di analisi indipendenti. L'efficacia del modello è stata comprovata da VirusTotal sin da agosto 2016 e ha ricevuto punteggi molto alti in altri test indipendenti, come quelli condotti dagli NSS Labs. In tutte le occasioni, il modello si è dimostrato estremamente efficace, pur restituendo un numero esiguo di falsi positivi.

"Uno dei migliori punteggi in termini di performance che siano mai stati raggiunti nei nostri test".
Maik Morgenstern, CTO, AV-TEST

Performance: La tecnologia di deep learning di Sophos è rapidissima. In meno di 20 millisecondi, il modello è stato in grado di estrarre milioni di funzionalità da un file, condurre un'analisi approfondita e determinare se tale file fosse innocuo o malevolo. L'intero processo ha avuto luogo prima dell'esecuzione del file.

SophosLabs: Uno degli aspetti più importanti per qualsiasi modello sono i dati che sono stati utilizzati per la sua analisi. Il nostro team di esperti di data science è parte del gruppo SophosLabs, per cui ha accesso a centinaia di milioni di campioni. Grazie a questi dati, possiamo creare nei nostri modelli le migliori previsioni possibili. L'integrazione tra i due gruppi di esperti ha anche permesso una migliore classificazione dei dati (e di conseguenza anche la realizzazione di un modello più efficiente). La condivisione bidirezionale di dati di intelligence sulle minacce e di feedback del mondo reale tra i team di esperti di data science e i ricercatori in ambito di minacce migliora continuamente la precisione dei nostri modelli.

"Intercept X ha bloccato tutti gli attacchi complessi e avanzati che le abbiamo lanciato contro"
ESG Lab Report, dicembre 2017

Effettuate subito una prova gratuita

Registratevi per una prova gratuita di 30 giorni su: sophos.it/interceptx

Vendite per l'Italia:
Tel: (+39) 02 94 75 98 00
E-mail: sales@sophos.it

02/01/18 DS IT (2897-DD)

SOPHOS